What is claimed is:

Sub a1

1. A method for generating an authentication tag for a message that can be used for error correction comprising:

processing a portion of the message using a reversible first function to produce an intermediate result; and

processing the intermediate result with a second function to produce the authentication tag.

2. The method of claim 1, further comprising encrypting the intermediate result.

3. The method of claim 2, further comprising sending the intermediate result to a receiver of the message.

4. The method of claim 3, further comprising sending the authentication tag to the receiver.

5. A method for detecting errors in a message comprising:

receiving at least one message data word and an authentication tag, said authentication tag produced from said at least one message data word according to a nested message authentication code having a reversible inner function ;

processing said received at least one message data word according to said nested message authentication code to produce an authentication tag;

determining whether said produced authentication tag is the same as said received authentication tag.

6. The method of claim 5, wherein said receiving comprises receiving at least one message data word, an authentication tag, and an intermediate result from said reversible inner function.

7. The method of claim 5, wherein said receiving comprises receiving at least one message data word, an authentication tag, and an encrypted intermediate result from said reversible inner function.

8. The method of claim 7, further comprising decrypting said encrypted intermediate result if said produced authentication tag is not the same as said received authentication tag.

9. The method of claim 7, wherein said processing comprises processing said received at least one message data word according to said nested message authentication code to produce an authentication tag and an intermediate result from said reversible inner function.

10. The method of claim 9, further comprising determining whether said decrypted intermediate result is the same as said produced intermediate result.

11. The method of claim 10, further comprising correcting an erroneous message data word if said decrypted intermediate result is not the same as said produced intermediate result.

12. The method of claim 10, wherein said correcting comprises identifying said erroneous message data word using a reverse inner function corresponding to said reversible inner function.